Lesson Module Status

- Slides – draft
- Properties - done
- Flashcards – not done
- 1st minute quiz –
- Web Calendar summary –
- Web book pages – done
- Commands –
- Howtos –
- Skills pacing -
- Lab – done
- Depot (VMs) – na

Course history and credits

Jim Griffin

- Jim created the original version of this course
- Jim's site: http://cabrillo.edu/~jgriffin/

Rick Graziani

- Thanks to Rick Graziani for the use of some of his great network slides
- Rick's site: http://cabrillo.edu/~rgraziani/

CIS 192 – Lesson 13

Joe A.

Joe P.

www.cccconfer.org
dial-in: 888-886-3951
passcode: 439080

John

Junious

Robert

Kay

Chuck

Lieven

Rich

Jesus

Josh

Edgar

Joe B.

Chris H.

Edwin

Julio

Jack

Brynden

Casady

Ryan

VMs for tonight

(Revert, 384MB RAM and Power up)

Celebrian

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

The LAST Quiz

Please take out a blank piece of paper, switch off your monitor, close your books, put away your notes and answer these questions:

- What port is used by an IMAP server?
- Is sendmail more of a (DA) Delivery Agent or a (MTA) Mail Transport Agent?
- What record types are used in DNS to route email over the Internet?

Network Information Service

Objectives	Agenda
• Install and configure NIS to serve common system files to domain clients	• Quiz • Questions on previous material • Housekeeping • Troubleshooting SLO Assessment • NIS • Review for Test 3 • Wrap

Questions on previous material

Questions?

- Previous lesson material
- Lab assignment

VM Screen Resolution

Steps to increase screen resolution on VMware VM:

1. In run level 3 (text mode)
2. Edit **/etc/X11/xorg.conf** and add these lines to the end:

```
Section "Monitor"
    Identifier "vmware"
EndSection
```

3. Run **vmware-config-tools.pl**
   no to vmhgfs module
   no to vmxnet module
   yes to change guest X resolution
   3 for 1024x768

4. **service network restart**
5. **startx** or **init 5**

The Evolution configuration windows are too big when using the 800x600 screen size

fetchmail

fetchmail

- Fetches mail from remote Access Agents (POP and IMAP servers) that can then be read by a local MUA like /bin/mail.
- See http://fetchmail.berlios.de/
- Fetchmail is configured for each user with a .fetchmailrc file in their home directory.
- Read your mail locally using /bin/mail

fetchmail

- Example 1 - Hershey

```
$ cd
$ chmod 400 .fetchmailrc
$ cat .fetchmailrc
poll hershey protocol pop3
username lastname
password password
keep
```

*the **keep** option, will keep messages on the server (by not flushing them) after downloading*

```
$ fetchmail
fetchmail: Server CommonName mismatch: localhost.localdomain != hershey
fetchmail: Server certificate verification error: self signed certificate
fetchmail: Server certificate verification error: certificate has expired
1 message (1 seen) for rich at hershey (631 octets).
skipping message rich@hershey:1 not flushed
```

By default, fetchmail will only pull down new messages and skip messages that were previously downloaded

fetchmail

- Example 2 - hayrocket.com

```
$ cd;
$ chmod 400 .fetchmailrc;
$ cat .fetchmailrc
poll mail.hayrocket.com protocol pop3
username firstname@hayrocket.com
password password
fetchall
keep
```

*the **fetchall** option will download all messages, even those that already have been viewed*

```
$ fetchmail
fetchmail: Server CommonName mismatch: *.mail.dreamhost.com != mail.hayrocket.com
fetchmail: Server certificate verification error: unable to get local issuer certificate
fetchmail: Server certificate verification error: certificate not trusted
fetchmail: Server certificate verification error: unable to verify the first certificate
4 messages for rich@hayrocket.com at mail.hayrocket.com (9151 octets).
reading message rich@hayrocket.com@mail.hayrocket.com:1 of 4 (1170 octets). not flushed
reading message rich@hayrocket.com@mail.hayrocket.com:2 of 4 (2315 octets).. not flushed
reading message rich@hayrocket.com@mail.hayrocket.com:3 of 4 (3076 octets)... not flushed
reading message rich@hayrocket.com@mail.hayrocket.com:4 of 4 (2590 octets).. not flushed
```

No messages skipped, all were read (downloaded)

fetchmail

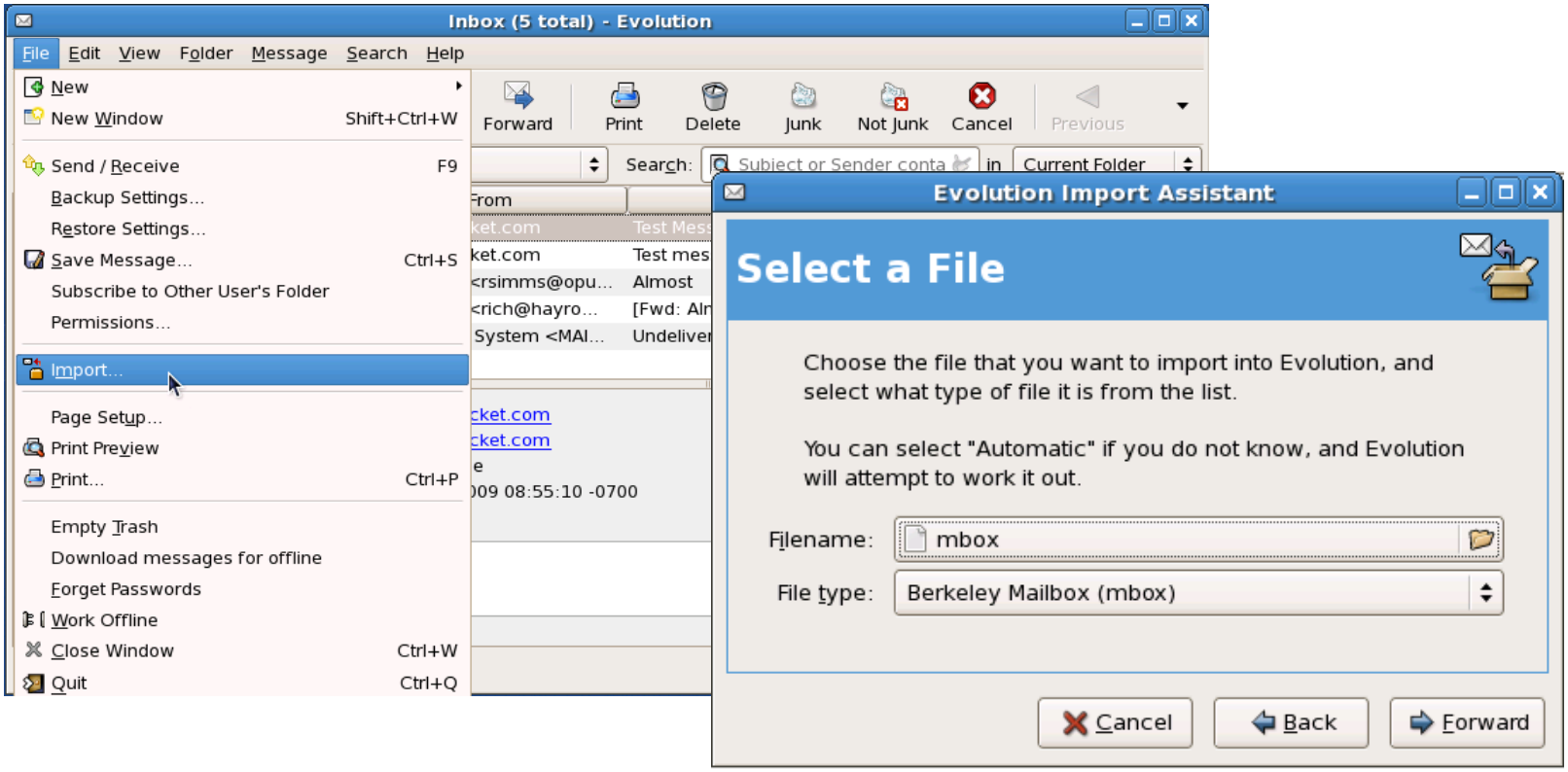
- Use /bin/mail to read your messages

/bin/mail is the name of the program that is run when you use the mail command

```
You have mail in /var/spool/mail/cis192
[cis192@arwen ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/cis192": 4 messages 4 unread
>U  1 rsimms@opus.cabrillo  Sun May 10 07:18  34/1607  "Almost"
 U  2 rich@hayrocket.com    Sun May 10 07:18  61/2689  "[Fwd: Almost]"
 U  3 MAILER-DAEMON@nehi.d  Sun May 10 07:18 100/3457  "Undelivered Mail Returned to"
 U  4 rich@hayrocket.com    Sun May 10 07:18  71/2954  "[Fwd: Test Message]"
& 1
Message 1:
From rsimms@opus.cabrillo.edu  Sun May 10 07:18:33 2009
X-Original-To: rich@hayrocket.com
Delivered-To: rsimms@spaceymail-mx2.g.dreamhost.com
Date: Sun, 3 May 2009 17:16:55 -0700
From: Rich Simms <rsimms@opus.cabrillo.edu>
To: daniel@hayrocket.com, denise@hayrocket.com, doug@hayrocket.com,
        fred@hayrocket.com, greg@hayrocket.com, john@hayrocket.com,
        jonathan@hayrocket.com, kayla@hayrocket.com, kyle@hayrocket.com,
        lou@hayrocket.com, marc@hayrocket.com, rich@hayrocket.com,
        tyler@hayrocket.com, wes@hayrocket.com
Subject: Almost

there ...

& x
[cis192@arwen ~]$
```

fetchmail

- Or import your messages into another MUA



Save messages from /bin/mail to a mailbox file (like mbox) and import that file into an MUA like Evolution.

application "ping"

Not Really … but I wish

- The ping command tests connectivity between nodes.
- There is no real “application ping”
- However, the telnet command can be used in a way to "ping an application"
- Examples:

telnet mx.cruzio.com 25
telnet mail.hayrocket.com 110
telnet mail.hayrocket.com 143
telnet simms-teach.com 80

Note: The Cabrillo firewall blocks outgoing connections to port 110 and 143.

For testing in building 2500 connect to Hershey at 172.30.N.20 (N=1 for classroom and 4 for the lab) instead. Hershey, will accept connections on port 25, 110 and 143

Check SMTP Server (port 25)

Checking for a SMTP application

```
[root@elrond ~]# telnet hershey 25
Trying 172.30.4.20...
Connected to hershey (172.30.4.20).
Escape character is '^]'.
220 hershey.MiddleEarth.net ESMTP Sendmail 8.12.8/8.12.8; Tue, 12 May 2009
08:38:58 -0700
quit
221 2.0.0 hershey.MiddleEarth.net closing connection
Connection closed by foreign host.
[root@elrond ~]#

[root@elrond ~]# telnet mail.hayrocket.com 25
Trying 208.113.200.50...
Connected to mail.hayrocket.com (208.113.200.50).
Escape character is '^]'.
220 spaceymail-a3.g.dreamhost.com ESMTP
quit
221 Bye
Connection closed by foreign host.
```

Using Elrond VM in room 2504 CIS Lab

Check POP Server (port 110)

Checking for a POP application

```
[root@elrond ~]# telnet mail.hayrocket.com 110
Trying 208.113.200.50...
telnet: connect to address 208.113.200.50: Connection refused
telnet: Unable to connect to remote host: Connection refused


[root@elrond ~]# telnet hershey 110
Trying 172.30.4.20...
Connected to hershey (172.30.4.20).
Escape character is '^]'.
+OK POP3 [172.30.4.20] v2001.78rh server ready
quit
+OK Sayonara
Connection closed by foreign host.
```

Cabrillo firewall blocks outgoing connections to pop servers

Check IMAP Server (port 143)

Checking for a IMAP application

```
[root@elrond ~]# telnet mail.hayrocket.com 143
Trying 208.113.200.50...
telnet: connect to address 208.113.200.50: Connection refused
telnet: Unable to connect to remote host: Connection refused
[root@elrond ~]#
```

```
[root@elrond ~]# telnet hershey 143
Trying 172.30.4.20...
Connected to hershey (172.30.4.20).
Escape character is '^]'.
* OK [CAPABILITY IMAP4REV1 LOGIN-REFERRALS STARTTLS AUTH=LOGIN]
[172.30.4.20] IMAP4rev1 2001.315rh at Tue, 12 May 2009 08:41:03 -0700 (PDT)
a01 logout
* BYE hershey IMAP4rev1 server terminating connection
a01 OK LOGOUT completed
Connection closed by foreign host.
[root@elrond ~]#
```

Cabrillo firewall blocks outgoing connections to imap servers

Check Web Server (port 80)

Checking for a HTTP application

```
[root@elrond ~]# telnet simms-teach.com 80
Trying 208.113.161.13...
Connected to simms-teach.com (208.113.161.13).
Escape character is '^]'.
GET / HTTP/1.0
host: simms-teach.com

HTTP/1.1 200 OK
Date: Tue, 12 May 2009 23:30:28 GMT
Server: Apache/2.0.63 (Unix) PHP/4.4.7 mod_ssl/2.0.63 OpenSSL/0.9.7e
mod_fastcgi/2.4.2 Phusion_Passenger/2.0.6 DAV/2 SVN/1.4.2
X-Powered-By: PHP/5.2.6
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
        <head>
< snipped >
```

Don't forget to enter a blank line here

Check connectivity with some application services using **telnet *server port***

- mail.hyrocket.com (SMTP server at port 25)
  - Use: **telnet mail.hayrocket.com 25** *use **quit** to teminate*
- www.google.com (web server at port 80)
  - Use: **telnet google.com 80** *use **quit** to teminate*
- hershey (IMAP and POP server at ports 143 and 110)
  - Use: **telnet hershey 143** *use **a1 logout** to teminate*
  - Use: **telnet hershey 110** *use **quit** to teminate*

*Requires that **172.30.1.20 hershey** is in your /etc/hosts file*

Housekeeping

- Lab 9 due tonight
- Test 3 next week

Warmup

http://simms-teach.com/cis192home.php

Student Learner Outcomes

- Identify the protocols used for establishing connections between network nodes, as well as the common conventions used by each protocol.
- Install and configure a local area network (LAN) that meets the resource needs of a small to medium business.
- Install and configure common network client/server applications in a LAN environment.
- Assess and modify the performance of a network using both graphical and command line tools.
- Identify, isolate, and correct malfunctions in a computer network.

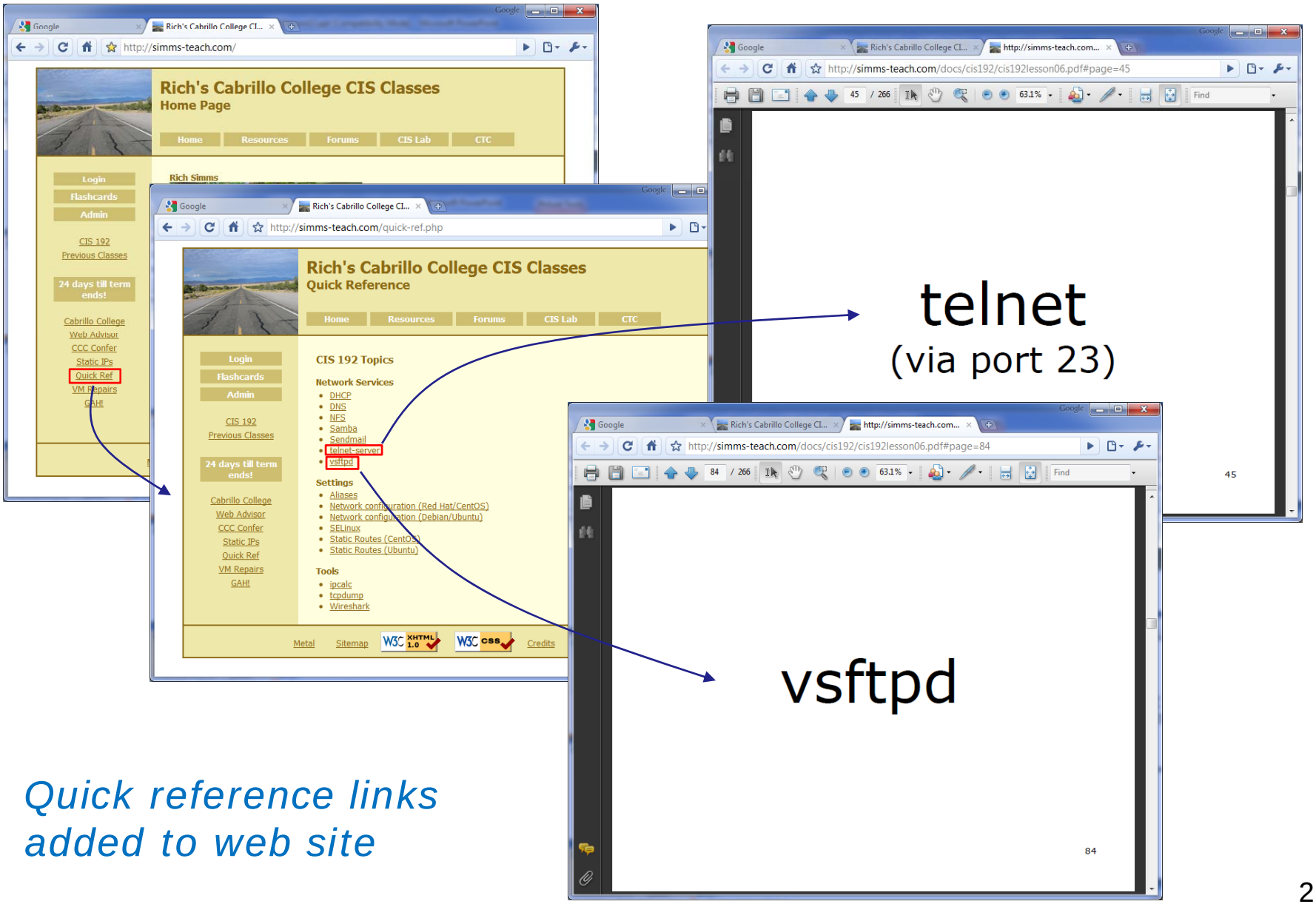
For our warm-up tonight we will assess the last SLO above

SLO: Identify, isolate, and correct malfunctions in a computer network

***The problem**: The FTP and Telnet services on Celebrian are no longer are available and customers are getting very upset.*

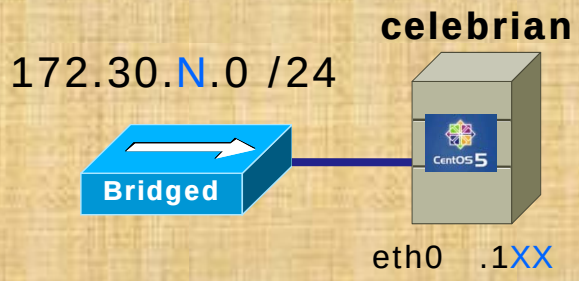
***History**: The server was shutdown to replace a noisy fan. However after the server was started up again both the Telnet and FTP services stopped working.*

***Situation**: the original administrator who configured telnet and vsftpd the server has left the company. As a consultant you have just signed a Professional Services Agreement get both these services back online.*



Quick reference links added to web site

Troubleshooting Assessment



.1XX is based on your station number and the IP Table
N=1 for the classroom and N=4 for the CIS lab or CTC
http://simms-teach.com/docs/static-ip-addrs.pdf

- Revert and power-up Celebrian
- Cable as shown
- Use **dhclinet eth0** for an initial IP address
- **scp *logname*@opus.cabrillo.edu:/home/cis192/scripts/down* .**
- **chmod 700 download-scripts-packages** (use tab complete)
- **./download-scripts-packages** (and download everything)
- **cd bin**
- **./do-act13A-celebrian**
- Repair the problem with Telnet and FTP services
- Verify your fix by accessing these services from another VM

NIS Overview

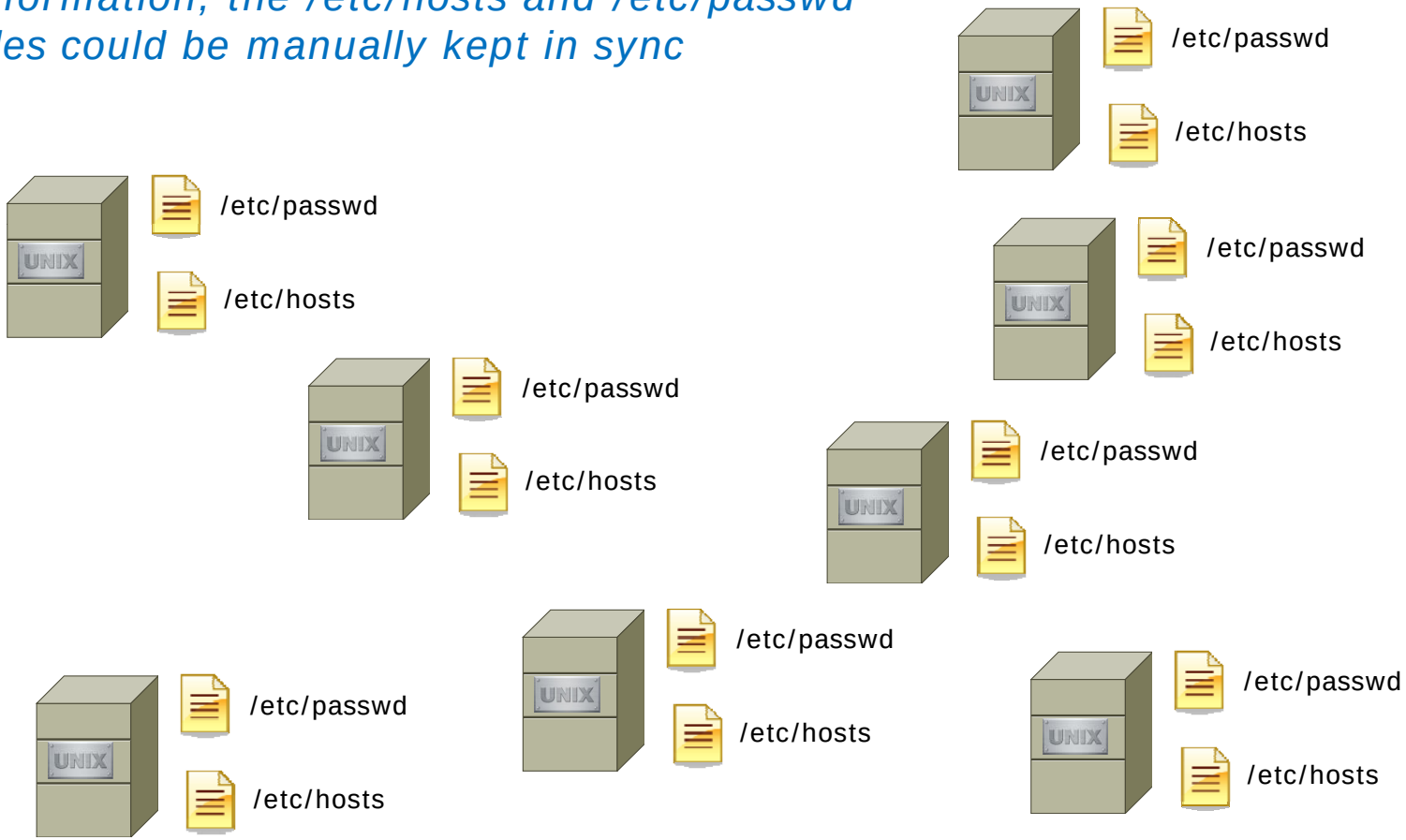
Network Information Service (NIS)

This lecture is about the Network Information Service (NIS). NIS allows centralization of system configuration files like /etc/hosts and /etc/passwd for use by other systems in an organization.

Based on Jim Griffin's Lesson #10 on Configuring Email at:
- http://cabrillo.edu/~jgriffin/CIS192/files/lesson10.html

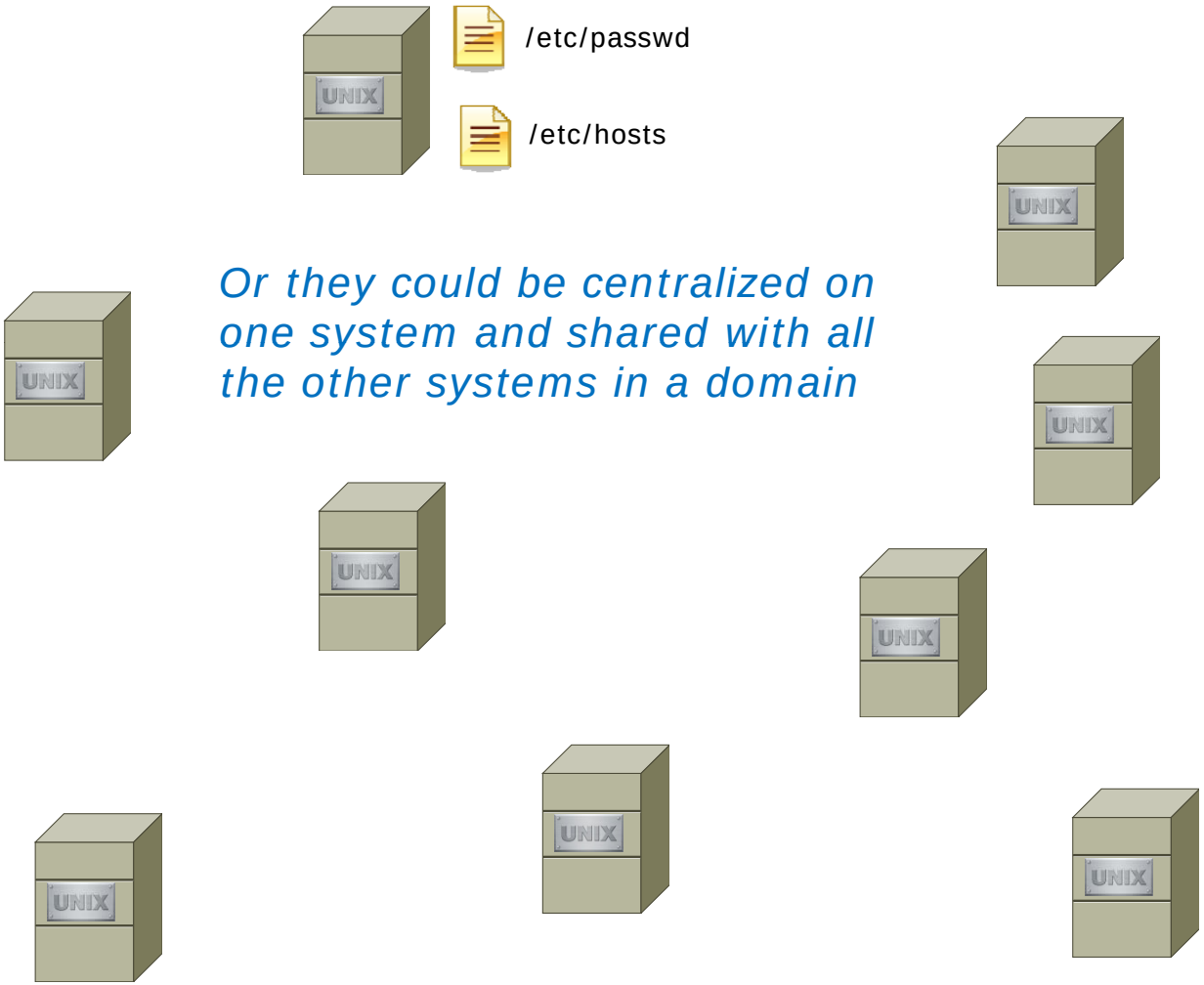
Network Information Service (NIS)

To have common host and account information, the /etc/hosts and /etc/passwd files could be manually kept in sync



Requiring a great deal of administration effort

Network Information Service (NIS)



Or they could be centralized on one system and shared with all the other systems in a domain

Requiring far less system administration effort

Network Information Service (NIS)

- Allows system configuration information files to be shared across multiple systems
- Developed and licensed by SUN Microsystems
- NIS and NFS (Network File System) are independent and configured separately
- Originally known as Yellow Pages and that is why the file names start with yp
- Follows a client-server architecture
- Based on RPC (Remote Procedure Call) based and uses the port mapper (portmap)
- Analogous to the Windows domain system although internally completely different.
- NIS can run over TCP or UDP

Network Information Service (NIS)

Client-Server Operations

- NIS operates within a domain defined by an NISDOMAIN name.
- This name should not be the same as the DNS domain.
- An NIS server, serves ASCII text UNIX database files to clients by compiling them into a DBM format for faster queries.
- The database files may include the following:
  - /etc/passwd
  - /etc/group
  - /etc/hosts
  - /etc/networks
  - /usr/lib/aliases
  - /etc/services
  - /etc/protocols
  - /etc/rpc
- The database files are called maps.
- All systems in the same NIS domain share the same set of maps.

Components

NIS Packages

- ypserv
  - the server daemon and its configuration file.

- ypbind
  - the client daemon and its configuration file.

- yp-tools
  - several client utilities including:

ypcat
dumps the content of a particular NIS map file

ypwhich
specifies the name of the NIS server you are using

ypmatch
like ypcat, but returns only specific key values

yppasswd
allows the user to change their password on the NIS server

Server side

Service Applications

Steps to installing services

1. Install software package using **yum**, **rpm** or build from source code
2. Customize service's configuration file
3. Modify the firewall to allow access to the service
4. Customize SELinux context settings to allow use
5. Start the service
6. Configure service to automatically start when system boots
7. Monitor and verify service is running
8. Troubleshoot as necessary
9. Monitor log files as appropriate
10. Configure additional security

Installing an NIS Server

Step 1 *Check software*

```
[root@arwen ~]# rpm -qa | grep ypserv
[root@arwen ~]# rpm -qa | grep ypbind
ypbind-1.19-12.el5
[root@arwen ~]# rpm -qa | grep yp-tools
yp-tools-2.9-0.1
[root@arwen ~]# rpm -qa | grep portmap
portmap-4.0-65.2.2.1
[root@arwen ~]#
```

server component is not installed

client package is installed

The tools package is already installed

NIS uses the portmapper which is also already installed

Installing NIS Server Files

Step 1 *Installing NIS server package (with yum)*

```
[root@arwen ~]# yum install ypserv
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * addons: centos.corenetworks.net
 * base: mirror.nyi.net
 * extras: ftp.ussg.iu.edu
 * updates: ftp.ussg.iu.edu
addons                                                  |  951 B     00:00
base                                                    | 2.1 kB     00:00
extras                                                  | 2.1 kB     00:00
updates                                                 | 1.9 kB     00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package ypserv.i386 0:2.19-5.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved
```

Installing NIS Server Files

Step 1 *Installing NIS server package*

```
================================================================================
 Package            Arch             Version                 Repository       Size
================================================================================
Installing:
 ypserv             i386             2.19-5.el5              base            134 k

Transaction Summary
================================================================================
Install       1 Package(s)
Update        0 Package(s)
Remove        0 Package(s)

Total download size: 134 k
Is this ok [y/N]: y
Downloading Packages:
ypserv-2.19-5.el5.i386.rpm                               | 134 kB     00:01
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
```

Installing NIS Server Files

Step 1 *Installing NIS server package*

```
Running Transaction
  Installing     : ypserv                                                  1/1

Installed:
  ypserv.i386 0:2.19-5.el5

Complete!
[root@arwen ~]#
```

Installing NIS Server Files

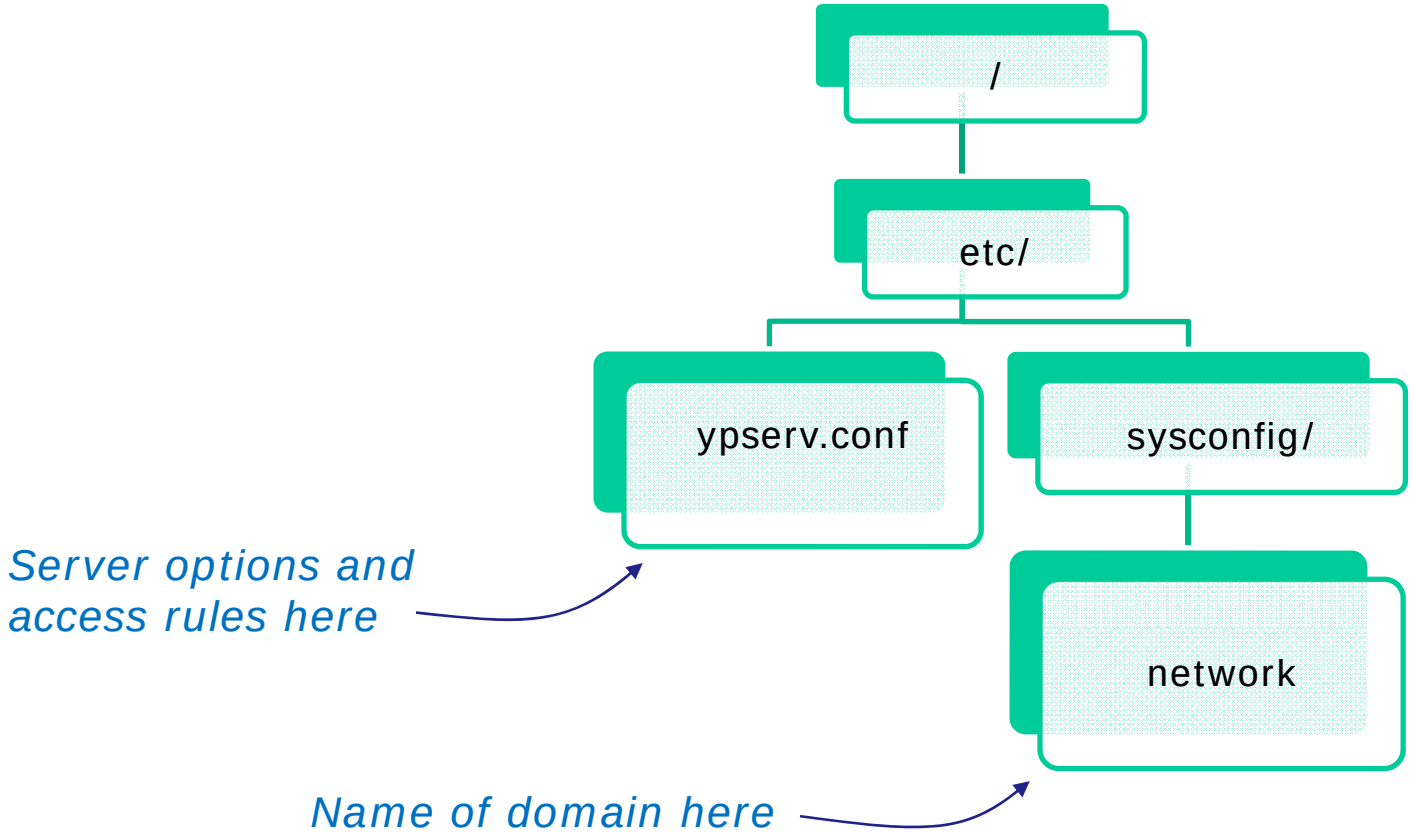
Step 1 *Installing NIS server package (with RPM)*

```
[root@arwen packages]# ls yp*
ypserv-2.19-5.el5.i386.rpm

[root@arwen packages]# rpm -Uhv ypserv-2.19-5.el5.i386.rpm
Preparing...                ########################################### [100%]
   1:ypserv                 ########################################### [100%]
[root@arwen packages]#
```

*Or using the **rpm** command*

NIS Server

Step 2 *Customize the configuration files*



Server-side NIS

/etc/ypserv.conf syntax *See **man ypserv.conf** for details*

```
option: <argument>                    # This is an option line
```

dns: no
files: 30
etc.

```
host : domain : map : security  # This is an access rule
```

none
port
deny

***
name

passwd.byname
passwd.byuid
hosts.byname
etc.

hostname or IP address
172.30.4.
172.30.4.0/255.255.255.0
***

Server-side NIS

```
[root@arwen bin]# cat /etc/ypserv.conf
#
# ypserv.conf   In this file you can set certain options for the NIS server,
#               and you can deny or restrict access to certain maps based
#               on the originating host.
#
#               See ypserv.conf(5) for a description of the syntax.
#

# Some options for ypserv. This things are all not needed, if
# you have a Linux net.

# Should we do DNS lookups for hosts not found in the hosts table ?
# This option is ignored in the moment.
dns: no

# How many map file handles should be cached ?
files: 30

# Should we register ypserv with SLP ?
slp: no
# After how many seconds we should re-register ypserv with SLP ?
slp_timeout: 3600

# xfr requests are only allowed from ports < 1024
xfr_check_port: yes
```

default ypserv.conf file

Server-side NIS

```
# The following, when uncommented,  will give you shadow like passwords.
# Note that it will not work if you have slave NIS servers in your
# network that do not run the same server as you.

# Host                      : Domain  : Map              : Security
#
# *                         : *       : passwd.byname    : port
# *                         : *       : passwd.byuid     : port

# Not everybody should see the shadow passwords, not secure, since
# under MSDOG everbody is root and can access ports < 1024 !!!
*                           : *       : shadow.byname    : port
*                           : *       : passwd.adjunct.byname : port

# If you comment out the next rule, ypserv and rpc.ypxfrd will
# look for YP_SECURE and YP_AUTHDES in the maps. This will make
# the security check a little bit slower, but you only have to
# change the keys on the master server, not the configuration files
# on each NIS server.
# If you have maps with YP_SECURE or YP_AUTHDES, you should create
# a rule for them above, that's much faster.
# *                         : *       : *                : none

[root@arwen bin]#
```

default ypserv.conf file

Server-side NIS

Setting up an NIS server

We will be using the default configuration file which looks like the following with all the comments stripped out

```
[root@arwen bin]# cat /etc/ypserv.conf | grep -v '^$' | grep -v '^ *#'
dns: no
files: 30
slp: no
slp_timeout: 3600
xfr_check_port: yes
*                       : *         : shadow.byname    : port
*                       : *         : passwd.adjunct.byname : port
```

do DNS lookups

how many data files should be cached

for service location protocol

forces NIS to run on privileged ports (<1024)

rules

Which hosts (=any)* : *The domain this rule to apply to (*=all)* : *The map (database) to be accessed* : *security:*
- *none=allow always*
- *port=allow (if port <1024)*
- *deny=no access*

Server-side NIS

Temporary but immediate setting

```
[root@arwen bin]# nisdomainname bittersweet
[root@arwen bin]#
```

Permanent setting

```
[root@ghiradelli ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=no
GATEWAY=172.30.1.1
HOSTNAME=ghiradelli.rivendell
NISDOMAIN=bittersweet
[root@ghiradelli ~]#
```

Specifying the NIS domain name bittersweet

NIS Server and the Firewall

Step 3 *Firewall*

Because NIS uses port mapper which uses random ports we will disable the firewall on the NIS server.

Configure your firewall rules on a gateway server instead for a protection barrier against outsiders.

NIS Server and SELinux

Step 4 *SELinux configuration*

Set permissive mode

```
[root@legolas ~]# setenforce permissive
[root@legolas ~]# getenforce
Permissive
```

Set enforcing mode

```
[root@legolas ~]# setenforce enforcing
[root@legolas ~]# getenforce
Enforcing
```

Show SELinux status

```
[root@legolas ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 21
Policy from config file:        targeted
```

No changes are needed for this lesson's activity

Keep SELinux in enforcing mode

NIS Server

Step 5 *Start the service*

```
[root@arwen bin]# service ypserv start
Starting YP server services:                               [  OK  ]
[root@arwen bin]#
```

Step 6 *Start the service automatically during system startup*

```
[root@arwen bin]# chkconfig ypserv on
[root@arwen bin]#
```

NIS Server

Step 7 *Monitor and verify service is running*

```
[root@arwen bin]# service ypserv status
ypserv (pid  10969) is running...
[root@arwen bin]#
```

NIS Server

Step 7 *Monitor and verify service is running*

```
[root@arwen bin]# netstat –tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:2049                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:705                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:840                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:782                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:854                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:920                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:42328               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
[root@arwen bin]#
```

There are a lot of TCP ports in use by NFS, NIS and Port Mapper

NIS Server

Step 7 *Monitor and verify service is running*

```
[root@arwen bin]# rpcinfo -p localhost | grep tcp
    100000    2   tcp    111  portmapper
    100024    1   tcp    705  status
    100007    2   tcp    782  ypbind
    100007    1   tcp    782  ypbind
    100011    1   tcp    840  rquotad
    100011    2   tcp    840  rquotad
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  42328  nlockmgr
    100021    3   tcp  42328  nlockmgr
    100021    4   tcp  42328  nlockmgr
    100005    1   tcp    854  mountd
    100005    2   tcp    854  mountd
    100005    3   tcp    854  mountd
    100004    2   tcp    920  ypserv
    100004    1   tcp    920  ypserv
[root@arwen bin]#
```

*User **rpcinfo** to see ports in use by NIS, NFS and Port Mapper*

NIS Server

Step 7 *Monitor and verify service is running*

```
[root@arwen bin]# netstat -uln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 0.0.0.0:2049                0.0.0.0:*
udp        0      0 0.0.0.0:779                 0.0.0.0:*
udp        0      0 0.0.0.0:37774               0.0.0.0:*
udp        0      0 0.0.0.0:917                 0.0.0.0:*
udp        0      0 0.0.0.0:935                 0.0.0.0:*
udp        0      0 0.0.0.0:936                 0.0.0.0:*
udp        0      0 0.0.0.0:699                 0.0.0.0:*
udp        0      0 0.0.0.0:702                 0.0.0.0:*
udp        0      0 0.0.0.0:837                 0.0.0.0:*
udp        0      0 0.0.0.0:851                 0.0.0.0:*
udp        0      0 0.0.0.0:53224               0.0.0.0:*
udp        0      0 0.0.0.0:5353                0.0.0.0:*
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 :::35102                    :::*
udp        0      0 :::5353                     :::*
[root@arwen bin]#
```

There are a lot of UDP ports in use by NFS, NIS and Port Mapper

NIS Server

Step 7 *Monitor and verify service is running*

```
[root@arwen bin]# rpcinfo -p localhost | grep udp
    100000    2   udp    111  portmapper
    100024    1   udp    702  status
    100007    2   udp    779  ypbind
    100007    1   udp    779  ypbind
    100011    1   udp    837  rquotad
    100011    2   udp    837  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  37774  nlockmgr
    100021    3   udp  37774  nlockmgr
    100021    4   udp  37774  nlockmgr
    100005    1   udp    851  mountd
    100005    2   udp    851  mountd
    100005    3   udp    851  mountd
    100004    2   udp    917  ypserv
    100004    1   udp    917  ypserv
    100009    1   udp    935  yppasswdd
[root@arwen bin]#
```

*User **rpcinfo** to see ports in use by NIS, NFS and Port Mapper*

Server-side NIS

Step 7B *Create and maintain the maps (databases)*

- Use current systems files or optionally the ones in /var/yp
  - Add to passwd from /etc/passwd any lines you want to share
  - Add to shadow from /etc/shadow any lines you want to share
  - Add to hosts from /etc/hosts any line you want to share

- **ypinit –m** – identifies master and slave servers and makes map files
- **make -C /var/yp** – makes or updates the map files

Step 7B *Initialize NIS server and create map files*

NIS Server

```
[root@arwen bin]#  /usr/lib/yp/ypinit -m
At this point, we have to construct a list of the hosts which will run NIS
servers.  ghiradelli.rivendell is in the list of NIS server hosts.  Please continue to add
the names for the other hosts, one per line.  When you are done with the
list, type a <control D>.
        next host to add:  ghiradelli.rivendell
        next host to add:       next host to add:
The current list of NIS servers looks like this:

ghiradelli.rivendell

Is this correct?  [y/n: y]  We need a few minutes to build the databases...
Building /var/yp/bittersweet/ypservers...
Running /var/yp/Makefile...
gmake[1]: Entering directory `/var/yp/bittersweet'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gmake[1]: Leaving directory `/var/yp/bittersweet'

ghiradelli.rivendell has been set up as a NIS master server.

Now you can run ypinit -s ghiradelli.rivendell on all slave server.
```

Map (database) files are created for each system file

For example, hosts.byname and hosts.byaddr hold domain wide hostname-IP pairs for name resolution

Step 7B *Initialize NIS server and create map files*

NIS Server

```
[root@ghiradelli ~]# make -C /var/yp
make: Entering directory `/var/yp'
gmake[1]: Entering directory `/var/yp/bittersweet'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gmake[1]: Leaving directory `/var/yp/bittersweet'
make: Leaving directory `/var/yp'
[root@ghiradelli ~]#
```

Map (database) files are created for each system file

NIS Server

Step 7B *Update map files when system information changes*

```
[root@arwen bin]# make -C /var/yp
gmake[1]: Entering directory `/var/yp/bittersweet'
Updating passwd.byname...

Updating passwd.byuid...
Updating group.byname...

Updating group.bygid...
Updating netid.byname...

gmake[1]: Leaving directory `/var/yp/bittersweet'
make: Leaving directory `/var/yp'
```

Maps must be updated every time one of the source files has been modified e.g. adding new users

NIS Server

Step 8 *Troubleshoot*

```
[root@celebrian ~]# service ypbind start
Turning on allow_ypbind SELinux boolean
Binding to the NIS domain:                                 [  OK  ]
Turning off allow_ypbind SELinux boolean.............      [FAILED]

[root@celebrian ~]#
```

Problem: Client cannot join (bind to) the NIS domain

Fix: Disable firewall of NIS server

NIS Server

Step 9 *Monitor log files*

```
[root@elrond cat /var/log/messages | grep yp
[root@arwen bin]# cat /var/log/messages | grep yp
May 12 22:36:07 arwen ypserv[10418]: WARNING: no securenets file found!
May 12 22:36:07 arwen ypserv[10418]: Support for SLP (line 20) is not compiled in.
May 12 22:36:07 arwen ypserv[10418]: Support for SLP (line 22) is not compiled in.
May 12 22:42:51 arwen ypserv[10969]: WARNING: no securenets file found!
May 12 22:42:51 arwen ypserv[10969]: Support for SLP (line 20) is not compiled in.
May 12 22:42:51 arwen ypserv[10969]: Support for SLP (line 22) is not compiled in.
May 12 22:43:05 arwen setsebool: The allow_ypbind policy boolean was changed to 1 by root
May 12 22:43:07 arwen ypbind: bound to NIS server ghiradelli.rivendell
[root@arwen bin]#
```

Network Information Service (NIS)

Step 10 *Additional security*

- NIS has security vulnerabilities
- Getting an NIS server to broadcast a fictitious account allows an attacker to access any domain system.
- RPC (Remote Procedure Call) spoofing - early versions of portmap allowed any program to register as an RPC server. Attackers could provide their own NIS services with their own login information.
- NIS spoofing - early versions of NIS allows an attacker to inject a fake ypserv daemon that would respond to local client ypbind requests. Or an attacker could run a rogue computer to respond to client ypbind network requests with the attackers login information.
- If attackers are not firewalled out they can request copies of the NIS map files and obtain account names and encrypted passwords.

Client Side

Client-side NIS

Configuring an NIS client:

Clients need to run a daemon as well since accessing files like /etc/passwd and /etc/hosts is a common and continual process.

- Setup the NIS domain name
  - Run the command **domainname** *name*
  - Set the variable NISDOMAIN=*name* in **/etc/sysconfig/network**

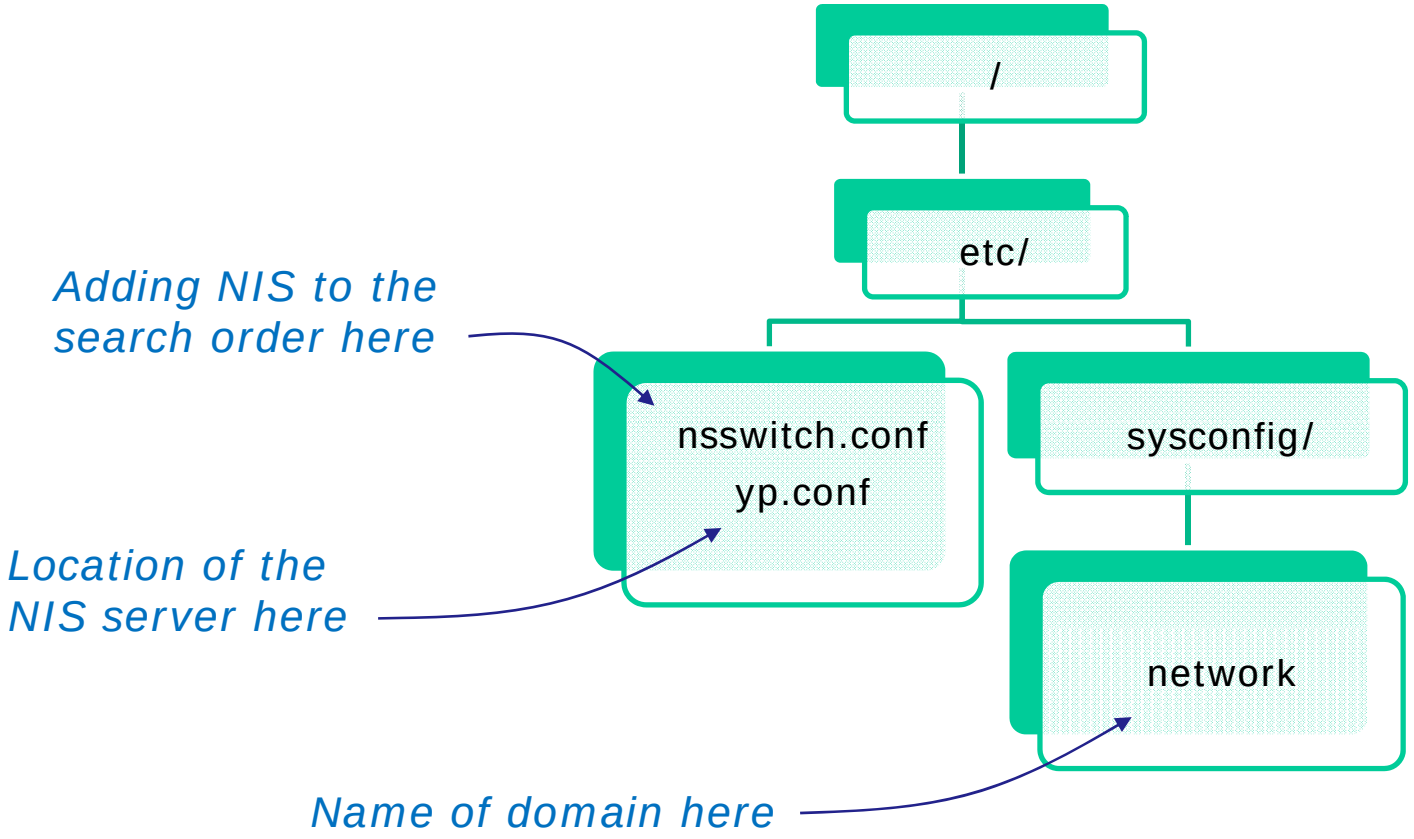
- Configure the **/etc/yp.conf** file using one of three syntaxes:
  - domain *name* server *hostname*
  - domain *name* broadcast
  - ypserver *name*

- Edit the **/etc/nsswitch.conf** file and add nis to the appropriate services

- Start the **ypbind** service

NIS Client

Step 2 *Customize the configuration files*



Ghiradelli Example

Client-side NIS

Set the NIS domain name

Temporary but immediate

```
[root@celebrian ~]# domainname bittersweet
[root@celebrian ~]# domainname
bittersweet
```

Permanent

```
[root@celebrian ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=celebrian.rivendell
NISDOMAIN=bittersweet
[root@celebrian ~]#
```

Client-side NIS

Configure the /etc/yp.conf file

```
[root@celebrian ~]# cat /etc/yp.conf
# /etc/yp.conf - ypbind configuration file
# Valid entries are
#
# domain NISDOMAIN server HOSTNAME
#       Use server HOSTNAME for the domain NISDOMAIN.
#
# domain NISDOMAIN broadcast
#       Use  broadcast  on  the local net for domain NISDOMAIN
#
# domain NISDOMAIN slp
#       Query local SLP server for ypserver supporting NISDOMAIN
#
# ypserver HOSTNAME
#       Use server HOSTNAME for the  local  domain.  The
#       IP-address of server must be listed in /etc/hosts.
#
# broadcast
#       If no server for the default domain is specified or
#       none of them is rechable, try a broadcast call to
#       find a server.
#
domain bittersweet server 172.30.1.200
```

Add this line

Client-side NIS

Edit the /etc/nsswitch.conf file and add nis to the appropriate services.

```
[root@celebrian ~]# cat /etc/nsswitch.conf
#
# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#       nisplus or nis+         Use NIS+ (NIS version 3)
#       nis or yp               Use NIS (NIS version 2), also called YP
#       dns                     Use DNS (Domain Name Service)
#       files                   Use the local files
#       db                      Use the local database (.db) files
#       compat                  Use NIS on compat mode
#       hesiod                  Use Hesiod for user lookups
#       [NOTFOUND=return]       Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:   files nis nisplus nis
#shadow:   files nis nisplus nis
#group:    files nis nisplus nis

passwd:     files nis
shadow:     files nis
group:      files nis

#hosts:     db files nisplus nis dns
hosts:      files dns

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

netgroup:   nisplus

publickey:  nisplus

automount:  files nisplus
aliases:    files nisplus

[root@celebrian ~]#
```

Modify these lines to include NIS

Client-side NIS

Start the NIS client (ypbind) service

```
[root@celebrian ~]# service ypbind start
Turning on allow_ypbind SELinux boolean
Binding to the NIS domain:                                 [  OK  ]
```

Note the SELinux setting is done automatically

Client-side NIS

Try it … you will like it!

```
[root@celebrian bin]# su - lopez
[lopez@celebrian ~]$ ls
lopez-file
[lopez@celebrian ~]$ cat /etc/passwd | grep lopez
[lopez@celebrian ~]$
```

Note the user does not show up in the local /etc/passwd file because they logged into the NIS domain instead

Join the cismud.net domain

Login as root on local VM

Use **dhclient eth0** to join the shire network

Add to /etc/hosts:

echo 172.30.1.20 hershey >> /etc/hosts

showmount -e hershey
mount hershey:/home /home

domainname cismud.net

Add to /etc/yp.conf:

domain cismud.net server hershey

Update /etc/nsswitch.conf lines:

passwd: files nis
hosts: files nis
group: files nis

service ypbind start

Login using your lastname as the account (either change to tty2 **[Ctrl-Alt-F2]** or use **su – lastname**)

Try after logging in:

ls
mount
cat /etc/password | grep $LOGNAME
exit
umount /home
service ypbind stop

Celebrian

Hershey

andes
armstrong
bobisuthi
collins
crivello
dahlin
hsieh
huberlantz
hutmacher
lee
lopez
mambulu
ordaz
ortega
prager
rivas
ross
saenz
unruh

Review

Test 3 material

- Lesson 9 - DNS
- Lesson 10 - NFS & Printing
- Lesson 11 - Samba
- Lesson 12 - Mail
- Lesson 13 - NIS

- Labs: 7 (DNS), 8 (Samba), 9 (email), X3 (NFS)

DNS

An Overview of Domain Name System

Paul worked at the Information Sciences Institute of the University of Southern California

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Can you imagine trying to keep these files updated on every single host in the world?

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Supports two type of queries:

- Recursive
- Iterative

In reality, the DNS is a huge, global distributed database spread across all the DNS servers in the world.

Each DNS server is authoritative for its own domain and maintains these forward and reverse lookup zones.

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

The client side of DNS. It initiates and sequences the queries that lead to the resolution of a name into an IP address

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Also known as the master server. This server maintains a database of hostname/IP pairs for the systems it serves. This server also provides authoritative answers for these same systems.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Also known as a slave server. This server is identical to the primary server except it does not maintain its own database. It's data is obtained instead from the primary server. Used as backup when the primary server is down and for load balancing.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Has no database of its own and does not obtain one from another server. Caching servers make queries on behalf of clients and cache the answers. Caching servers are used for performance reasons.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Contain the database resource records such as A records that map a hostname to a IP address, PTR records that map IP addresses to hostnames, NS records for name servers, and CNAME records for aliases.

Supports two type of queries:

- Recursive
- Iterative

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Supports two type of queries:

- Recursive
- Iterative

Provide either an answer or an error message

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Supports two type of queries:

- Recursive
- Iterative

Provide either an answer or a referral to another DNS server

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

Maintained by the Internet Systems Consortium: www.ics.org

An Overview of Domain Name System

Created in 1983 from the work led by Paul Mockapetris

Improves the deficiencies of the /etc/hosts file

DNS manages two databases (zones)

- Forward lookup zones: for mapping Domain names to IP addresses
- Reverse lookup zones: for mapping IP addresses to Domain names

Three components to DNS:

- Resolver
- The Server
  - Primary
  - Secondary
  - Caching
- Database files (db.domain-name)

Supports two type of queries:

- Recursive
- Iterative

This is what we will install and configure in Lab 7

Most popular implementation of DNS is Berkely Internet Name Daemon (BIND)

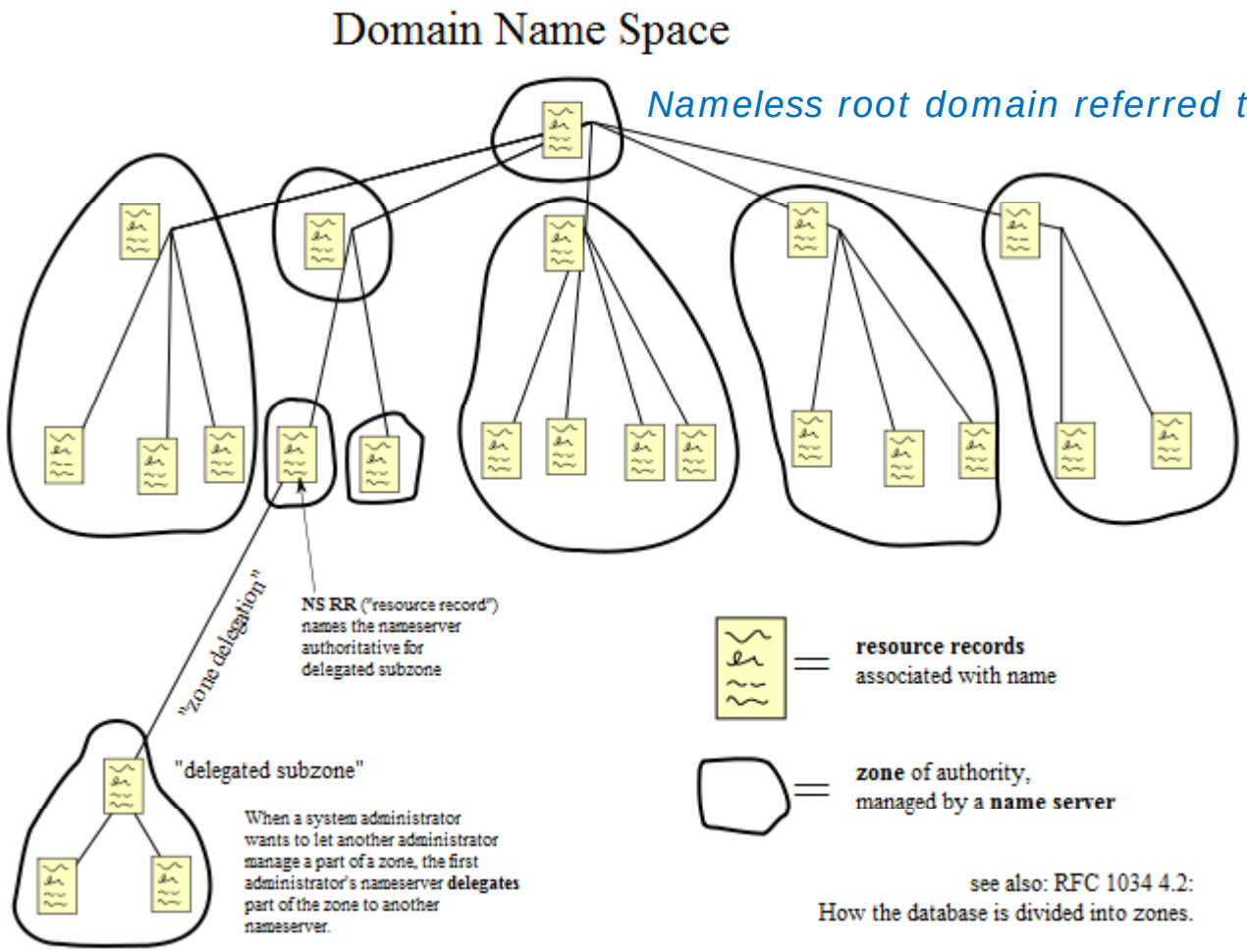
Maintained by the Internet Systems Consortium: www.ics.org

The DNS Namespace

- Top most domain in the namespace hierarchy is "."
- Top-level domains: .com, .net, .gov, .edu, .org .us, ...
- Special domain for reverse lookups: in-addr.arpa
- Fully Qualified Domain Names read from right to left
- Name registration was handled by InterNIC; now belongs to companies for profit.

InterNIC - Internet Network Information Center. Handled domain names and IP addresses prior to 1988 before getting turned over to ICANN

ICANN - Internet Corporation for Assigned Names and Numbers. ICANN accredits the domain name registrars (the companies that compete with other and register domain names)

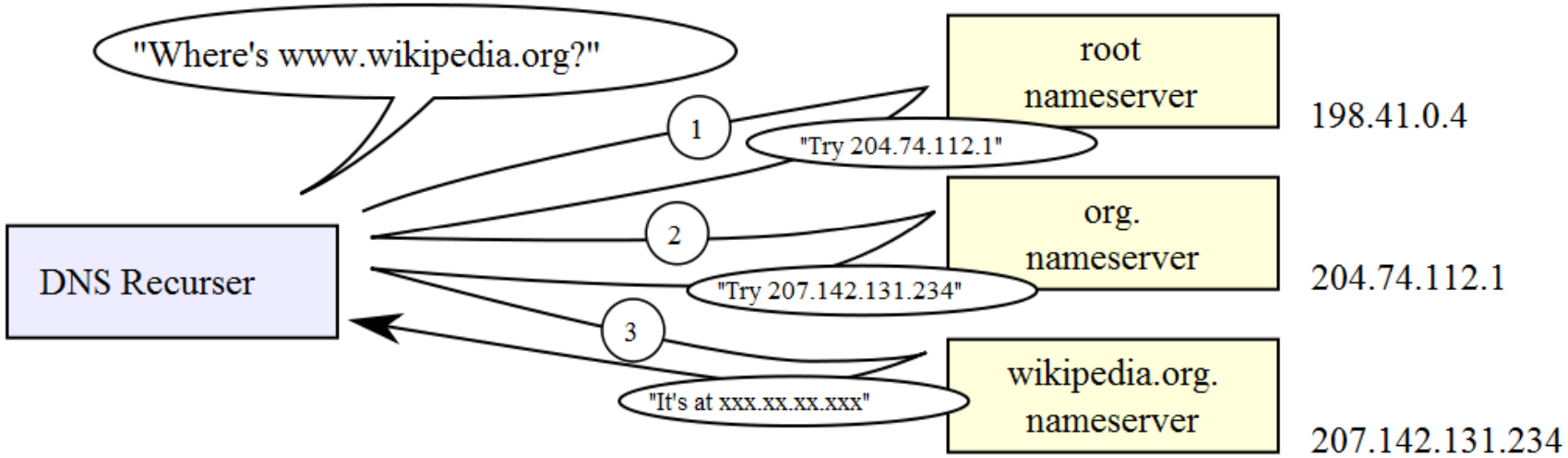


Nameless root domain referred to via "."

Generic TLD's - Top Level Domains (com, edu, net, org, mil, etc.)

Next level domains (e.g. hp.com, cabrillo.edu, yahoo.com, webhalks.org, etc.

source: http://en.wikipedia.org/wiki/File:Domain_name_space.svg



source: http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

DNS Database Resource Record types:

SOA - Start of Authority
NS - Nameserver
A - Address
PTR - Pointer (for reverse lookups)
CNAME – Aliases
MX – Mail server

DNS Installation and Configuration

Package names:	bind, caching-nameserver
Daemon name:	/usr/sbin/named
Startup script:	/etc/rc.d/init.d/named start or **service named start**
Database files:	/var/named/named.ca *IP address of root servers* /var/named/db.*in-addr*.arpa *reverse lookups* /var/named/db.*domain* name *forward lookups*
Configuration files:	/etc/named.conf *Overall configuration file* /etc/resolv.conf *DNS server to use* /etc/nsswitch.conf *Lookup order definition*

To reload configuration files: **rndc reload**

DNS

Situation: A local community college needs your help with their network. The college just installed a new classroom system, named station-24 however they cannot access it by name like they can with the other stations. They mention they have a DNS server named Hershey in a small closet but the student that configured it has left. The IP address for Hershey is 172.30.1.20.

They demonstrate the problem from one of their client systems:

```
[root@elrond ~]# host station24
station24.localdomain has address 172.30.1.224
```

```
[root@elrond ~]# host station25
Host station25 not found: 3(NXDOMAIN)
```

DNS

What are three ways you could fix this problem?

DNS

What are the pros and cons of each fix?

DNS

Lets check out one of the Linux clients first …

What is the name of the client DNS configuration file?

DNS

Lets check out Hershey …

What is the name of the DNS configuration file?

DNS

What do we need to find in this DNS configuration file?

DNS

DNS

How to we update DNS to add the IP address for station-24?

DNS

- `[root@elrond ~]# host station25`
  `station25.middleearth.net has address 172.30.1.125`

- `[root@elrond ~]# host 172.30.1.124`
  `125.1.30.172.in-addr.arpa domain name pointer station25.localdomain.`

Success!

Explore the DNS configuration on Hershey

Hershey

- Login to Hershey
- Find the main DNS configuration file and identify all the zones being handled by this DNS server.
- Looking at the main DNS configuration file what source port will Hershey use to contact other DNS servers?
- Find the forward lookup zone file for localdomain and locate the A records. Is there an A record for each station in room 2501?
- Find the reverse lookup zone file for 172.30.1.0 locate the PTR records
- Find the client DNS configuration file on Hershey. What is the search line and how does this search line help users do lookups?

```
andes
armstrong
bobisuthi
collins
crivello
dahlin
hsieh
huberlantz
hutmacher
lee
lopez
mambulu
ordaz
ortega
prager
rivas
ross
saenz
unruh
```

NFS

NFS

Situation: You've been hired a by a small company that produces riddles. They have a share used by the riddle engineers to keep all their riddles on. They have just purchased new system and can't remember how to set up this share on it. All they remember is that the master share is kept on their Hershey computer.

NFS

How do you show the directories being shared from Hershey?

NFS

How could you view those riddles on the new computer?

NFS

How could you make the remote share permanent?

Add a permanent NFS share

Elrond

- Work by yourself or with a neighbor
- Create a /riddles directory on Elrond
- Permanently mount the /riddles export on Hershey to your local /riddles directory. You will need to update /etc/fstab to do this.
- Restart Elrond and run both riddle scripts in /riddles

Printing

CUPS - Common UNIX Printing System
http://www.cups.org/

Packages
```
# yum install cups
# rpm -qa | grep cups
libgnomecups-0.2.2-8
cups-libs-1.2.4-11.18.el5_2.3
cups-1.2.4-11.18.el5_2.3
hal-cups-utils-0.6.2-5.2.el5
```

Firewall Ports Used
631/UDP
631/TCP

Configuration
```
http://localhost:631
```

Services and reloading configuration file changes
```
# service cups restart
Stopping cups:                                             [  OK  ]
Starting cups:                                             [  OK  ]
```

Printing

Situation: You are helping your Uncle Steve who works for a big software company in Washington state. He uses an HP superdome for his home PC. You have just installed CentOS 5.2 on this home system overwriting the previous OS that was installed. Now you need to configure the system so you can do remote printer management.

Printing

How do you determine if your current printer management software is running and then use it?

Printing

How would you enable this software to be used remotely?

Add a printer to Elrond

Elrond

- Browse to the web-based CUPS utility
- Add a pretend HP DesignJet 800PS on LPT #1
- Stop the printer but still allow jobs to be spooled (the Start Printer and Reject Jobs buttons should be showing on the Printers tab)
- Make this printer the default printer
- From the command line:
  - View available printers with **lpstat -p -d**
  - Print /etc/mtab with **lp /etc/mtab**
  - View the print queue with **lpq**
  - Remove the print job with **cancel #** (where # is job ID)

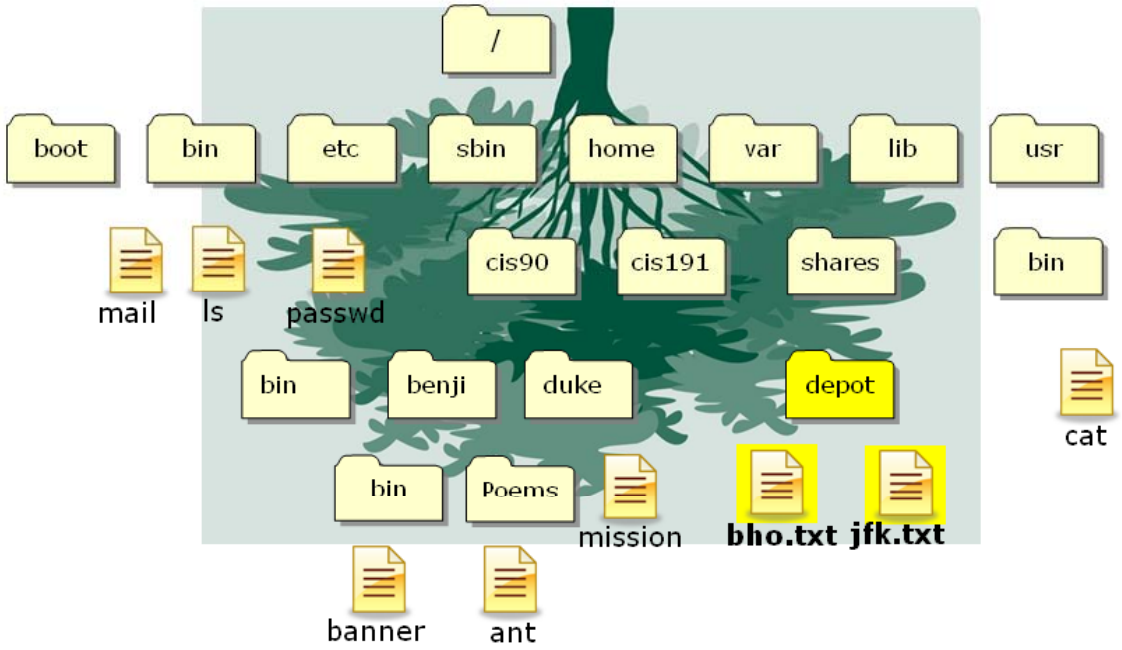
Samba

Samba

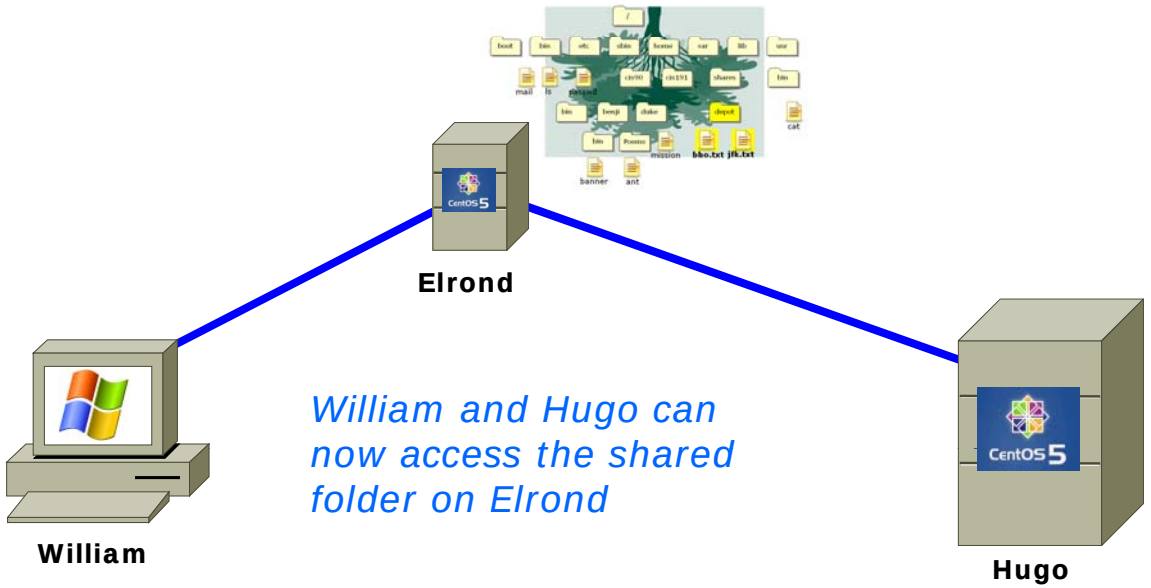
Elrond

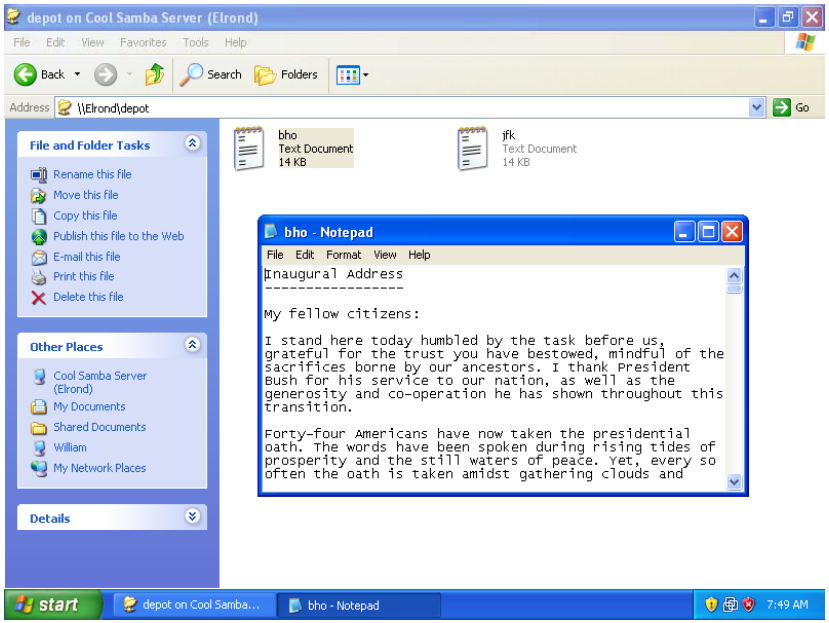
To make a share, add the following lines to ***/etc/samba/smb.conf*** *creates a shared directory on Elrond (and do a few other things)*

```
[depot]
        comment = Public files on Elrond
        path = /var/shares/depot
        read only = yes
        guest ok = yes
```



Samba






```
[root@hugo ~]# mount //elrond/depot /mnt
Password:
[root@hugo ~]# ls /mnt
bho.txt  jfk.txt
[root@hugo ~]# cd /mnt
[root@hugo mnt]# cat bho.txt
Inaugural Address
-----------------

My fellow citizens:

I stand here today humbled by the task
before us, grateful for the trust you
have bestowed, mindful of the sacrifices
```

www.samba.org

Packages

```
# rpm -qa | grep samba
samba-3.0.28-1.el5_2.1
samba-common-3.0.28-1.el5_2.1
samba-client-3.0.28-1.el5_2.1
```

Configuration

```
# ls /etc/samba/smb.conf
/etc/samba/smb.conf
```

Add user passwords

```
# smbpasswd -a lou
New SMB password:
Retype new SMB password:
Added user lou.
```

Firewall Ports Used

137/udp # NetBIOS Name Service
138/udp # NetBIOS Datagram Service
139/tcp # NetBIOS Session Service
445/tcp # Microsoft Directory Service

Browse shares

```
# smbclient -L hostname
# smbtree
```

Mount share

```
# mount //hostname/share /mount
```

SELinux context for shares

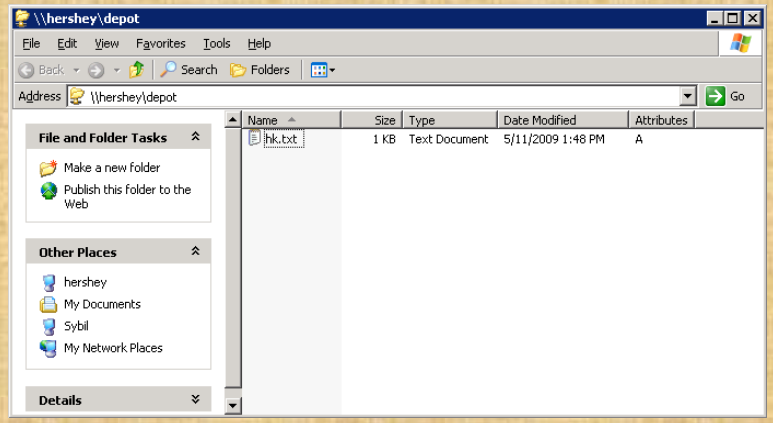
```
# chcon -Rv -t samba_share_t share
```

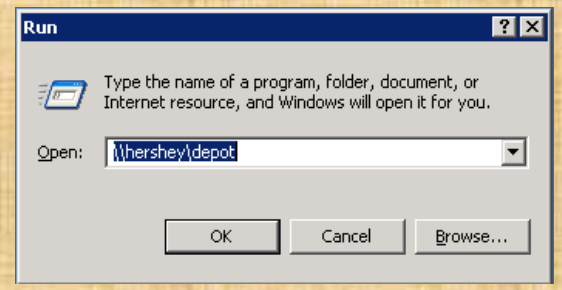
Services and reloading configuration file changes

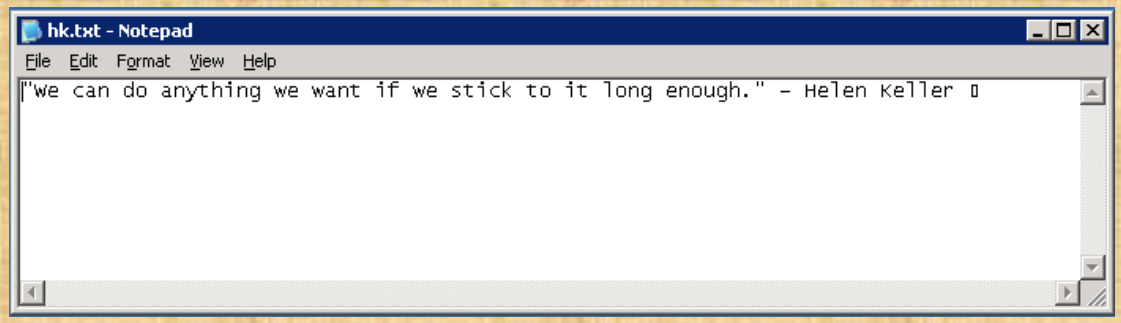
```
# service smb restart
Shutting down SMB services:                                [  OK  ]
Shutting down NMB services:                                [  OK  ]
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]
```

Samba

Situation: Everyone in the class can access the depot share on Hershey (\\hershey\depot) except for one student. Who can't log in and what troubleshooting steps need to be taken to resolve the issue?

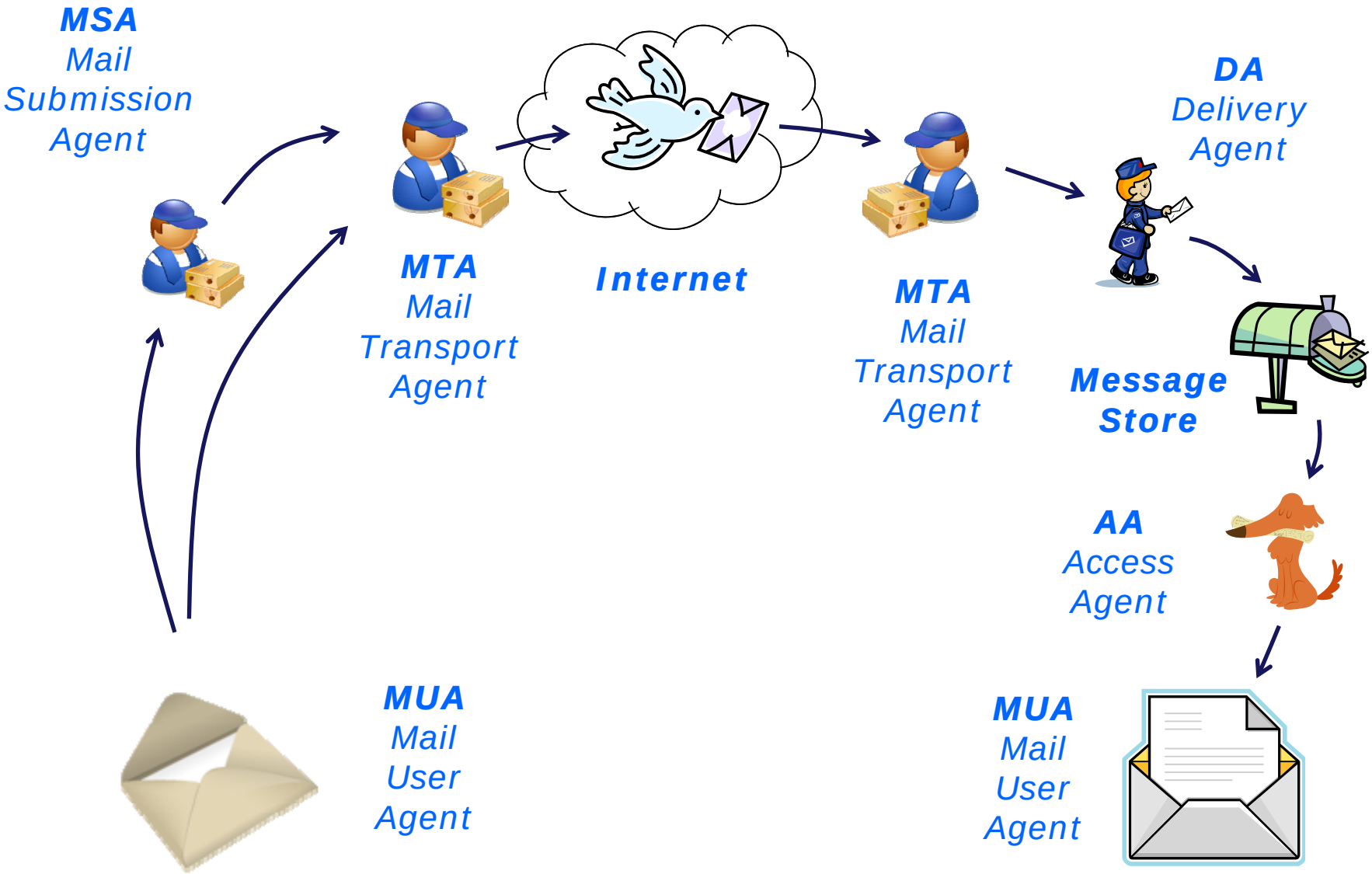






email

Overview of email



MSA
Mail Submission Agent

DA
Delivery Agent

Message Store

AA
Access Agent

MUA
Mail User Agent

compose and send message

MUA
Mail User Agent

open and read message

Overview of email

MSA
Mail Submission Agent

MTA
Mail Transport Agent

MUA
Mail User Agent

compose and send message

open and read message

Configuring the MTA (SMTP Server)

Identity | Receiving Email | Receiving Options | Sending Email | Defaults | Security

Server Type: SMTP

Description: For delivering mail by connecting to a remote mailhub using SMTP.

Server Configuration

Server: hershey

☑ Server requires authentication

Security

Use Secure Connection: No encryption

Authentication

Type: PLAIN | Check for Supported Types

Username: rich

☐ Remember password

Cancel | OK

Overview of email

MSA
Mail Submis Age

Configuring the AA (POP or IMAP Server)

Identity | Receiving Email | Receiving Options | Sending Email | Defaults | Security

Server Type: POP

Description: For connecting to and downloading mail from POP servers.

Configuration

Server: hershey

Username: rich

Security

Use Secure Connection: No encryption

Authentication Type

Password | Check for Supported Types

Remember password

Cancel | OK

A
il port nt

DA
Delivery Agent

Message Store

AA
Access Agent

MUA
Mail User Agent

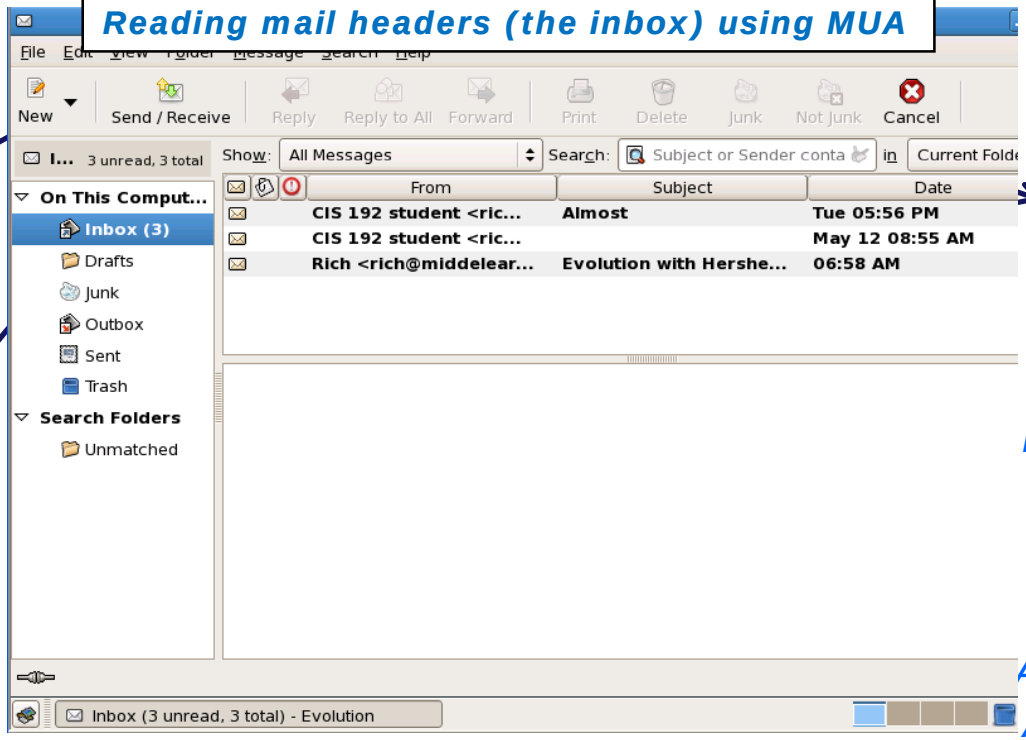
compose and send message

open and read message

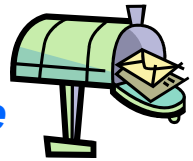
Overview of email

MSA
Mail Submission Agent

Reading mail headers (the inbox) using MUA



DA
Delivery Agent



Message Store

AA
Access Agent

MUA
Mail User Agent

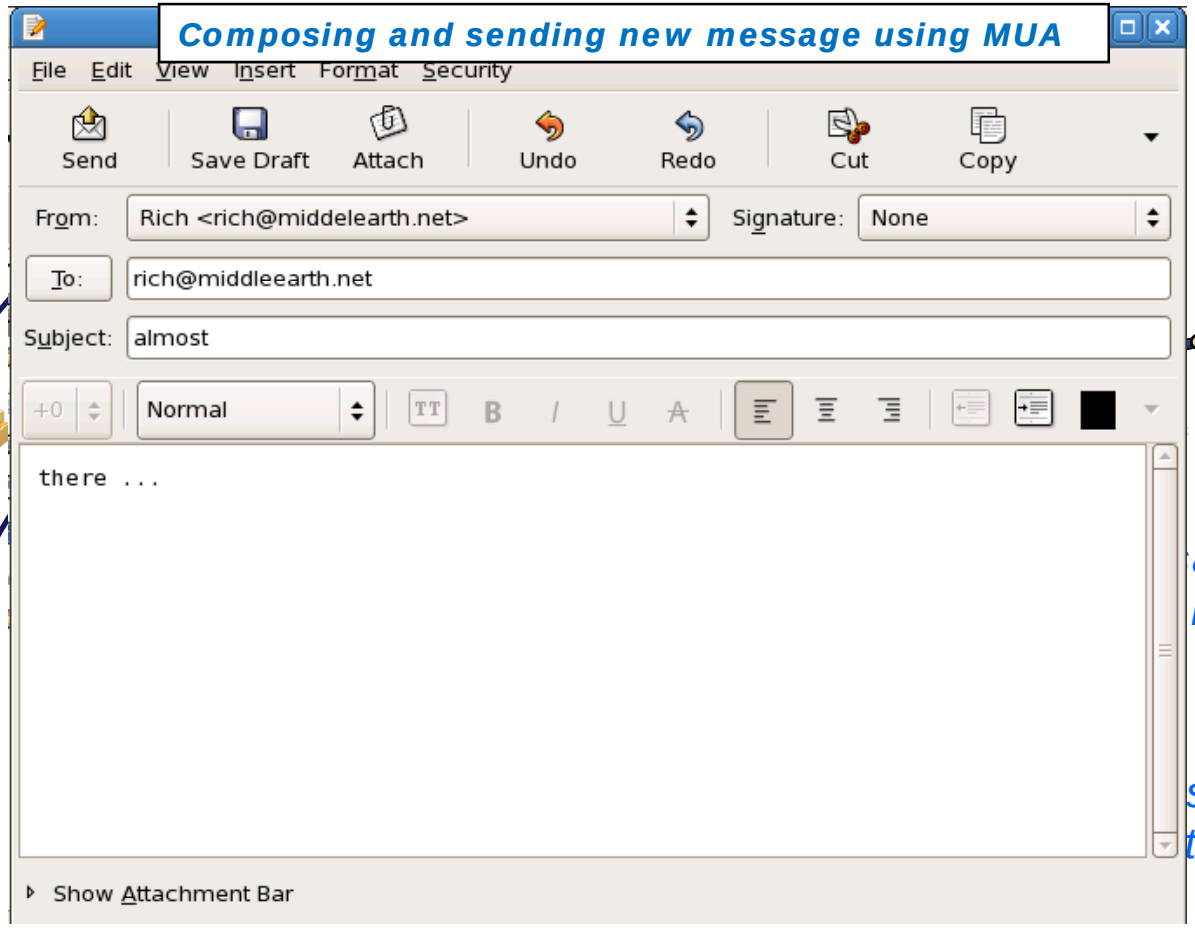
compose and send message

MUA
Mail User Agent

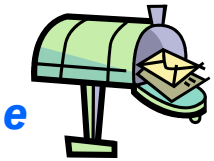
open and read message

Composing and sending new message using MUA

MSA
Mail
Submission
Agent



DA
Delivery
Agent

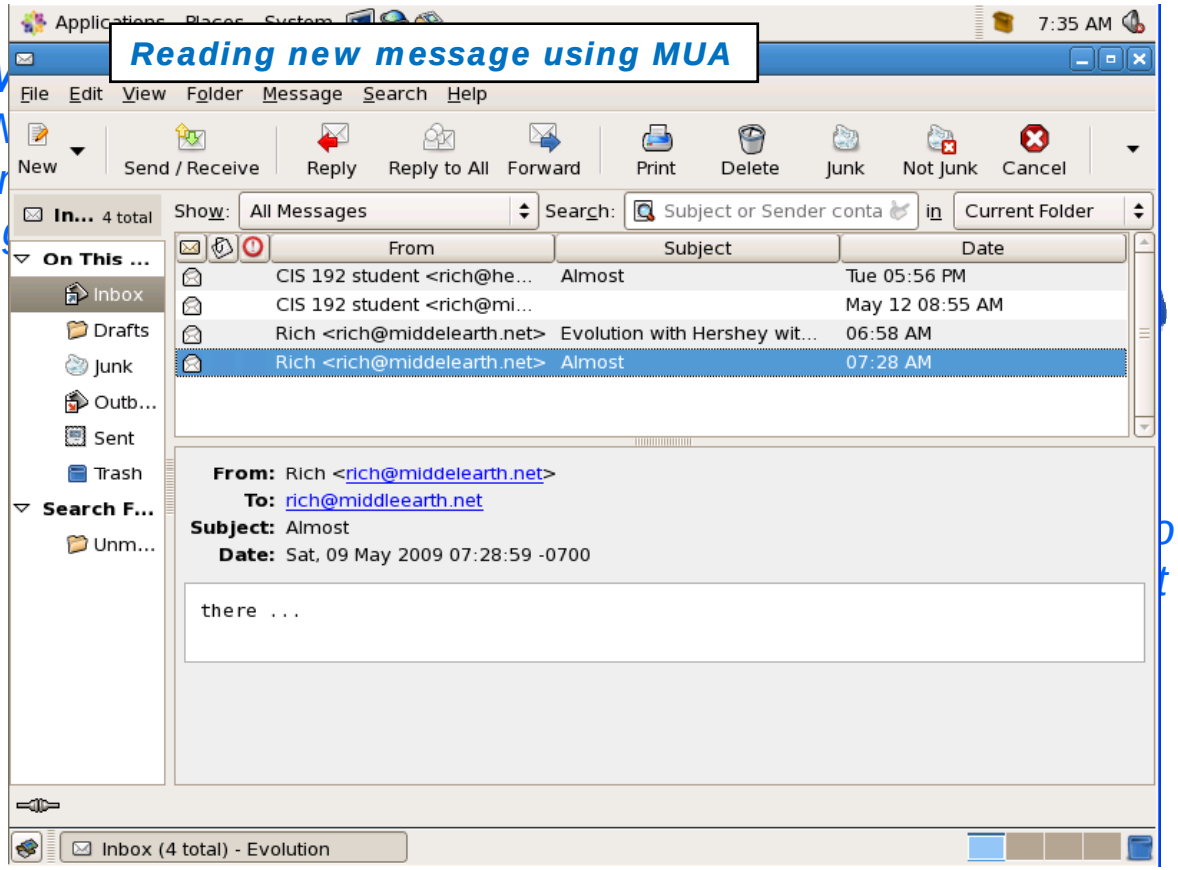


MUA
Mail
User
Agent

compose and send message

MUA
Mail
User
Agent

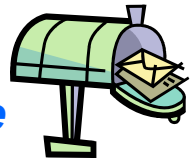
open and read message



MUA
Mail User Agent

compose and send message

DA
Delivery Agent



Message Store

AA
Access Agent

MUA
Mail User Agent

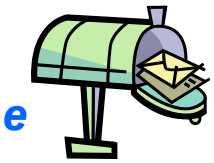
open and read message

Overview of email

```
[cis192@elrond ~]$ cat .fetchmailrc
poll hershey protocol pop3
username rich
password ********
keep
fetchall

[cis192@elrond ~]$ fetchmail
fetchmail: Server CommonName mismatch: localhost.localdomain != hershey
fetchmail: Server certificate verification error: self signed certificate
fetchmail: Server certificate verification error: certificate has expired
1 message for rich at hershey (548 octets).
reading message rich@hershey:1 of 1 (548 octets) not flushed

[cis192@elrond ~]$ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/cis192": 1 message
>   1 rich@middelearth.net  Sat May  9 07:29  24/941   "Almost"
& 1
Message 1:
From rich@middelearth.net  Sat May  9 07:29:23 2009
Subject: Almost
From: Rich <rich@middelearth.net>
To: rich@middleearth.net
Content-Type: text/plain
Date: Sat, 09 May 2009 07:28:59 -0700
Mime-Version: 1.0
X-Mailer: Evolution 2.12.3 (2.12.3-8.el5_2.3)
Content-Transfer-Encoding: 7bit

there …
```

Fetching from POP server and reading new message using another MUA (/bin/mail)

DA
Delivery Agent



compose and send message

open and read message

Mail Exercise

andes
armstrong
bobisuthi
collins
crivello
dahlin
hsieh
huberlantz
hutmacher
lee
lopez
mambulu
ordaz
ortega
prager
rivas
ross
saenz
unruh

- Configure the Evolution MUA on Elrond to read mail using the MTA (SMTP service) and AA (POP server) on Hershey

POP server: hershey
SMTP server: hershey
email ID: lastname**@middleearth.net**
Username: lastname

  - Configure messages to not be deleted on the server
  - Send yourself some emails

- Configure .fetchmailrc to pull your messages from hershey's pop service and read them with **/bin/mail** MUA

poll hershey protocol pop3
username firstname
password yourpassword
keep
fetchall

- Read one message saved on the pop server using **telnet**

telnet hershey 110
user firstname
pass yourpassword
list
retr 1
quit

Wrap

References

Jim Griffin

- http://www.cabrillo.edu/~jgriffin/CIS192/files/lesson10.html

Next Class

Assignment: Check Calendar Page
http://simms-teach.com/cis192calendar.php

Test 3 - Open book, notes, and computer:

- Lesson 9 - DNS
- Lesson 10 - NFS & Printing
- Lesson 11 - Samba
- Lesson 12 - Mail
- Lesson 13 - NIS

Backup

Classroom Static IP addresses for VM's

Station	IP	Static 1
Instructor	172.30.1.100	172.30.1.125
Station-01	172.30.1.101	172.30.1.126
Station-02	172.30.1.102	172.30.1.127
Station-03	172.30.1.103	172.30.1.128
Station-04	172.30.1.104	172.30.1.129
Station-05	172.30.1.105	172.30.1.130
Station-06	172.30.1.106	172.30.1.131
Station-07	172.30.1.107	172.30.1.132
Station-08	172.30.1.108	172.30.1.133
Station-09	172.30.1.109	172.30.1.134
Station-10	172.30.1.110	172.30.1.135
Station-11	172.30.1.111	172.30.1.136
Station-12	172.30.1.112	172.30.1.137

Station	IP	Static 1
Station-13	172.30.1.113	172.30.1.138
Station-14	172.30.1.114	172.30.1.139
Station-15	172.30.1.115	172.30.1.140
Station-16	172.30.1.116	172.30.1.141
Station-17	172.30.1.117	172.30.1.142
Station-18	172.30.1.118	172.30.1.143
Station-19	172.30.1.119	172.30.1.144
Station-20	172.30.1.120	172.30.1.145
Station-21	172.30.1.121	172.30.1.146
Station-22	172.30.1.122	172.30.1.147
Station-23	172.30.1.123	172.30.1.148
Station-24	172.30.1.124	172.30.1.149

Note the static IP address for your station to use in the next class exercise

Classroom DHCP IP allocation pools table by station number

Station	IP	Start	End
01	172.30.1.101	172.30.1.50	172.30.1.54
02	172.30.1.102	172.30.1.55	172.30.1.59
03	172.30.1.103	172.30.1.60	172.30.1.64
04	172.30.1.104	172.30.1.65	172.30.1.69
05	172.30.1.105	172.30.1.70	172.30.1.74
06	172.30.1.106	172.30.1.75	172.30.1.79
07	172.30.1.107	172.30.1.80	172.30.1.84
08	172.30.1.108	172.30.1.85	172.30.1.89
09	172.30.1.109	172.30.1.90	172.30.1.94
10	172.30.1.110	172.30.1.95	172.30.1.99
11	172.30.1.111	172.30.1.200	172.30.1.204
12	172.30.1.112	172.30.1.205	172.30.1.209

Station	IP	Start	End
13	172.30.1.101	172.30.1.210	172.30.1.214
14	172.30.1.102	172.30.1.215	172.30.1.219
15	172.30.1.103	172.30.1.220	172.30.1.224
16	172.30.1.104	172.30.1.225	172.30.1.229
17	172.30.1.105	172.30.1.230	172.30.1.234
18	172.30.1.106	172.30.1.235	172.30.1.239
19	172.30.1.107	172.30.1.240	172.30.1.244
20	172.30.1.108	172.30.1.245	172.30.1.249
21	172.30.1.109	172.30.1.250	172.30.1.254
22	172.30.1.110	172.30.1.30	172.30.1.34
23	172.30.1.111	172.30.1.35	172.30.1.39
24	172.30.1.112	172.30.1.20	172.30.1.44
Instruct	172.30.1.100	172.30.1.45	172.30.1.49

Use these pools of addresses based on your station number to avoid conflicts on the classroom network

Example Hershey

Server-side NIS

Example: hershey

```
[root@hershey yp]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=hershey.MiddleEarth.net
NISDOMAIN=cismud.net
GATEWAY=172.30.1.1
```

```
[root@hershey root]# domainname
cismud.net
[root@hershey root]#
```

The NIS domain name on supported by Hershey is cismud.net

(Microsoft, Unix and Database classes)

Server-side NIS

Example: hershey

This file gets converted into database format

```
[root@hershey yp]# cat /var/yp/passwd
cis191:x:191:191:CIS191 Account:/home/cis191/cis191:/bin/bash
cis192:x:192:192:CIS192 Account:/home/cis192/cis192:/bin/bash
rsimms:x:749:100:Rich Simms:/home/rsimms:/bin/bash
daniel:x:1114:1114:CIS 192 student:/home/daniel:/bin/bash
denise:x:1115:1115:CIS 192 student:/home/denise:/bin/bash
doug:x:1116:1116:CIS 192 student:/home/doug:/bin/bash
fred:x:1117:1117:CIS 192 student:/home/fred:/bin/bash
john:x:1118:1118:CIS 192 student:/home/john:/bin/bash
jonathan:x:1119:1119:CIS 192 student:/home/jonathan:/bin/bash
kayla:x:1120:1120:CIS 192 student:/home/kayla:/bin/bash
kyle:x:1121:1121:CIS 192 student:/home/kyle:/bin/bash
lou:x:1122:1122:CIS 192 student:/home/lou:/bin/bash
marc:x:1123:1123:CIS 192 student:/home/marc:/bin/bash
tyler:x:1124:1124:CIS 192 student:/home/tyler:/bin/bash
wes:x:1125:1125:CIS 192 student:/home/wes:/bin/bash
greg:x:1126:1126:CIS 192 student:/home/greg:/bin/bash
rich:x:1127:1127:CIS 192 student:/home/rich:/bin/bash
[root@hershey yp]#
```

Server-side NIS

Example: hershey

```
[root@hershey yp]# cat /var/yp/hosts
172.30.1.100            instructor station-00
172.30.1.10             snickers
172.30.4.101            cis-lab-01
172.30.4.102            cis-lab-02
172.30.4.103            cis-lab-03
172.30.4.104            cis-lab-04
172.30.4.105            cis-lab-05
172.30.4.106            cis-lab-06
172.30.4.107            cis-lab-07
172.30.4.108            cis-lab-08
172.30.4.109            cis-lab-09
172.30.4.110            cis-lab-10
172.30.4.111            cis-lab-11
172.30.4.112            cis-lab-12
172.30.4.101            station-01
172.30.4.102            station-02
[root@hershey yp]#
```

This file gets converted into database format

Server-side NIS

Example: hershey

```
[root@hershey yp]# touch passwd
[root@hershey yp]# touch hosts


[root@hershey yp]# make -C /var/yp
make: Entering directory `/var/yp'
gmake[1]: Entering directory `/var/yp/cismud.net'
Updating passwd.byname...
Updating passwd.byuid...
Updating hosts.byname...
Updating hosts.byaddr...
gmake[1]: Leaving directory `/var/yp/cismud.net'
make: Leaving directory `/var/yp'
[root@hershey yp]#
```

The make will convert any modified files into database format

Server-side NIS

Example: hershey

These are the host and passwd database map files produced form the ASCII text host and passwd files

```
[root@hershey yp]# ls -l /var/yp/cismud.net/{host*,pass*}
-rw-------    1 root     root         12917 May  9 16:52 /var/yp/cismud.net/hosts.byaddr
-rw-------    1 root     root         13001 May  9 16:52 /var/yp/cismud.net/hosts.byname
-rw-------    1 root     root         13781 May  9 18:13 /var/yp/cismud.net/passwd.byname
-rw-------    1 root     root         13769 May  9 18:13 /var/yp/cismud.net/passwd.byuid
[root@hershey yp]#
```

```
[root@hershey yp]# file /var/yp/cismud.net/{host*,pass*}
/var/yp/cismud.net/hosts.byaddr:  GNU dbm 1.x or ndbm database, little endian
/var/yp/cismud.net/hosts.byname:  GNU dbm 1.x or ndbm database, little endian
/var/yp/cismud.net/passwd.byname: GNU dbm 1.x or ndbm database, little endian
/var/yp/cismud.net/passwd.byuid:  GNU dbm 1.x or ndbm database, little endian
[root@hershey yp]#
```

.byaddr = database indexed by address
.byname = database indexed by name
.byuid = database indexed by UID

Server-side NIS

Example: hershey

```
[root@hershey yp]# cat /etc/ypserv.conf

dns: no                    option ignored according to comment
files: 30                  the number of files to cache
xfr_check_port: yes        if yes NIS server must run on port < 1024

# Host                      : Domain  : Map              : Security
172.30.4.0/255.255.255.0 : *       : passwd.byname    : none
172.30.4.0/255.255.255.0 : *       : passwd.byuid     : none
172.30.4.                  : *       : hosts.byname     : none

172.30.1.0/255.255.255.0 : *       : passwd.byname    : none
172.30.1.0/255.255.255.0 : *       : passwd.byuid     : none
172.30.1.                  : *       : hosts.byname     : none
```

Make the passwd file (with shadow passwords merged in) and hosts map available to classroom and lab stations.

Server-side NIS

Example: hershey

Start or restart the NIS service

```
[root@hershey root]# service ypserv restart
Stopping YP server services:                               [  OK  ]
Starting YP server services:                               [  OK  ]
[root@hershey root]#
```

Start or restart the NIS password service

```
[root@hershey root]# service yppasswdd restart
Stopping YP passwd service:                                [  OK  ]
Starting YP passwd service:                                [  OK  ]
[root@hershey root]#
```

Join the bittersweet domain

Celebrian

Ghiradelli

Login as root on local VM

Add to /etc/yp.conf:

echo 172.30.1.200 ghiradelli >> /etc/hosts

showmount -e ghiradelli
mount ghiradelli:/home /home

domainname bittersweet

Add to /etc/yp.conf:

domain bittersweet server ghiradelli

Update /etc/nsswitch.conf lines:

passwd: files nis
hosts: files nis
group: files nis

service ypbind start

Login using your lastname as the account (either change to tty2 **[Ctrl-Alt-F2]** or use **su – lastname**)

Try after logging in:

ls
mount
cat /etc/password | grep $LOGNAME
exit
umount /home
serv

```
andes
armstrong
bobisuthi
collins
crivello
dahlin
hsieh
huberlantz
hutmacher
lee
lopez
mambulu
ordaz
ortega
prager
rivas
ross
saenz
unruh
```